CLAIMS

1. A method of authenticating a computer user comprising unlocking a secure media using a user entered identification, retrieving authentication credentials for the user from the secure media, the authentication credentials including a password, verifying the authentication credentials and, on successful verification, authenticating the user.

2. A method according to claim 1, wherein the retrieval of authentication credentials comprises retrieving the credentials from a vault.

3. A method according to claim 2, wherein the vault is located on the secure media.

4. A method according to claim 3, wherein the secure media is a smart card.

5. A method according to claim 2, wherein the vault is a secure file.

6. A method according to any preceding claim comprising changing the password stored as part of the authentication credentials on the secure media without disclosing the new password to the user.

7. A method according to claim 6, wherein changing the password comprises generating a random password in response to a change password request, authenticating the new password and storing the new password on the secure media, when authenticated as part of the user's authentication credentials.

8. A method according to claim 6 or 7, wherein the password is changed in response to a request generated

by the computer operating system or an application running on the computer.

9. A method according to claims 7 or 8, wherein the change password request is generated by the user.

10. A method according to any preceding claim comprising running a password recovery process if the authentication credentials are not verified, the password recovery process comprising assigning a one-time password to the user, submitting the authentication credentials including the assigned one time password, authenticating the user, generating a change password request, generating a new password in response to the change password request, and updating the secure media with the new password.

11. A method according to claim 10, wherein the new password is a random password.

12. A method according to any preceding claim, wherein the authentication permits user access to a computer system, wherein secure media is unlocked by the system graphical identification and authentication module (GINA) an the authentication credentials are retrieved by the GINA from the secure media and passed to the computer operating system for verification as part of the operating system logon procedure.

13. A method according to claim 7 and 12, wherein the new random password is generated by the GINA and sent by the GINA to the operating system logon procedure, and, when authenticated, the GINA causes the new random password to be stored in the secure media.

14. A method according to claim 13, wherein the new password is generated by the GINA and authenticated by the computer operating system.

15. A method according to any of claims 1 to 11, wherein the authentication permits user access to an application running on a computer system comprising generating scripts corresponding to application authentication requests.

16. A method according to claim 15, wherein the script generation comprises navigating the application to an authentication screen, selecting the authentication screen, generating a script corresponding to the application screen, testing the generated script and saving the script.

17. A method according to claim 15 or 16, comprising distributing the script to one or more users of the application to which it relates.

18. A method according to claim 17 comprising loading the script at a computer to which the script has been distributed.

19. A method according to any of claims 15 to 18, comprising learning user credentials for the application, the user credentials including a password.

20. A method according to claim 19, wherein the learning of user credentials comprises running the generated script, detecting an application authentication screen, querying the secure media for authentication credentials for the application, reading authentication credentials submitted by the user if no credentials are found for the application on the secure media, retrieving the submitted credentials

from the screen and, on authentication of the end user, saving the credentials at the secure media.

21. A method according to claim 20, comprising replaying the stored authentication credentials on subsequent attempts to open the application by the user.

22. A method according to claim 21, wherein the replaying of user credentials comprises detecting the application authentication screen, retrieving the authentication credentials from the secure media, populating the authentication screen with the authentication credentials and submitting the authentication screen to the application.

23. A method according to any of claims 15 to 22, comprising detecting a password change screen relating to the application, generating a new random password, submitting the new password to the application, and, on detection of completion of the password change, storing the new password at the secure media.

24. A method according to claim 23, wherein the new password is submitted to the application with the old password.

25. A method according to any of claims 15 to 24, comprising displaying an application authentication screen to the user when authentication credentials retrieved from the secure media are rejected by the application, receiving correct authentication credentials from the user, submitting the authentication screen with the correct authentication credentials to the application, and on authentication, storing the correct credentials in the secure media.

26. A method according to claim 25, comprising temporarily storing the correct authentication credentials when the credentials are submitted to the application.

27. A computer readable storage medium having stored thereon computer readable code which when run on a computer causes the computer to perform the method of any of claims 1 to 26.

28. A computer or computer network programmed to perform the method of any of claims 1 to 26.

29. Apparatus for authenticating a computer user comprising a secure media having user authentication credentials including a password stored therein, means for unlocking the secure media via a user entered identification and retrieving the credentials and means for verifying the credentials and, on verification, authenticating the user.

30. Apparatus according to claim 29, wherein the secure media includes a vault for storing the authentication credentials.

31. Apparatus according to claim 30, wherein the secure media is a smart card and the means for unlocking the secure media includes a smart card reader.

32. Apparatus according to claim 30, wherein the vault comprises a secure file.

33. Apparatus according to any of claims 29 to 32, where the means for unlocking the secure media further comprises means for changing the user password without disclosing the new password to the user.

34. Apparatus according to claim 33, wherein the means for changing the password includes a random password generator responsive to a change password request, and where the means for including the secure media comprises means for storing the new password in the secure media on authentication of the new password.

35. Apparatus according to any preceding claim wherein the authentication permits user access to a computer system, and the means for unlocking the secure media comprises a Graphical Identification and Authentication Module (GINA) arranged to retrieve authentication credentials from the secure media and pass them to the operating system of the computer system for verification as part of the operating system logon procedure.

36. Apparatus according to claim 35, wherein the GINA includes the random password generator, means for sending the newly generated password to the operating system for authentication, means for temporarily storing the new password and means for causing the new password to be stored in the secure media on verification by the operating system.

37. Apparatus according to any of claim 29 to 34, wherein the authentication permits user access to an application on a computer system, comprising a script generator for generating scripts corresponding to application requests.

38. Apparatus according to claim 37, wherein the script generator comprises means for navigating the application to an authentication screen, means for selecting the authentication screen, means for generating a script corresponding to the

authentication screen, means for testing the generated script and a store for storing the script.

39. Apparatus according to claim 37 or 38, comprising means for distributing the script to one or more computers using the applications to which the script relates.

40. Apparatus according to claim 39, comprising means at a computer to which the script is distributed for loading the script.

41. Apparatus according to any of claims 37 to 40, comprising a scripting module including means for learning user credentials for an application including a password.

42. Apparatus according to claim 41, wherein the learning means comprises means for running the loaded script, means for detecting an application authentication screen, means for querying the secure media for authentication credentials for the application, means for reading authentication credentials submitted by the user if no credentials are found at the secure media, means for retrieving the submitted credentials and means for saving the credentials at the secure media.

43. Apparatus according to claim 42, comprising means for replaying the stored authentication credentials on subsequent attempts to open the application by the user.

44. Apparatus according to any of claims 37 to 43 comprising a temporary store for new passwords prior to authentication and storage in the secure media.

45. A computer including apparatus according to any of claims 29 to 44 for authenticating a user to the computer of an application running on the computer.

46. A computer network including apparatus according to any of claims 29 to 44 for authenticating a user to the network or to an application running on the network.

47. Apparatus for authenticating a user to a computer network comprising a secure media at a network computer, the secure media storing authentication credentials including a password stored therein, a GINA program for unlocking the secure media in response to a user PIN, the GINA further comprising code for retrieving the authentication credentials from the secure media and passing them to the computer or network operating system for verification.

48. Apparatus according to claim 47, wherein the GINA further includes code for detecting a password change request from the operating system, for generating a new random password in response to the request, for passing the new password to the operating system and, on authentication of the new password, storing the new password in the secure media as part of the authentication credentials.

49. Apparatus for authenticating a user of an application running on a computer or a computer network, comprising a secure media at the computer or a user computer on the network, the secure media storing authentication credentials including a password stored therein, a scripting module for unlocking the secure module in response to a user PIN, the scripting module further comprising code for retrieving the

authentication credentials from the secure media and passing them to the application for verification.

50. Apparatus according to claim 49, wherein the scripting module includes code for detecting a password change screen generated by the application, code for generating a new random password in response to the screen, code for passing the new password to the application and, on authentication of the new password, code for causing the storage media to store the new password as part of the authentication credentials.